IPAの提案する デジタルテレビにおけるセキュリティ対策検討ガイドの紹介

独立行政法人情報処理推進機構（IPA）
セキュリティセンター
情報セキュリティ技術ラボラトリー　研究員
金野　千里　（博士（理学））

2011．2．24

1. はじめに

2. 情報家電のセキュリティにおける課題と解決の方向性

3. デジタルテレビにおけるセキュリティ対策検討ガイド

4. おわりに

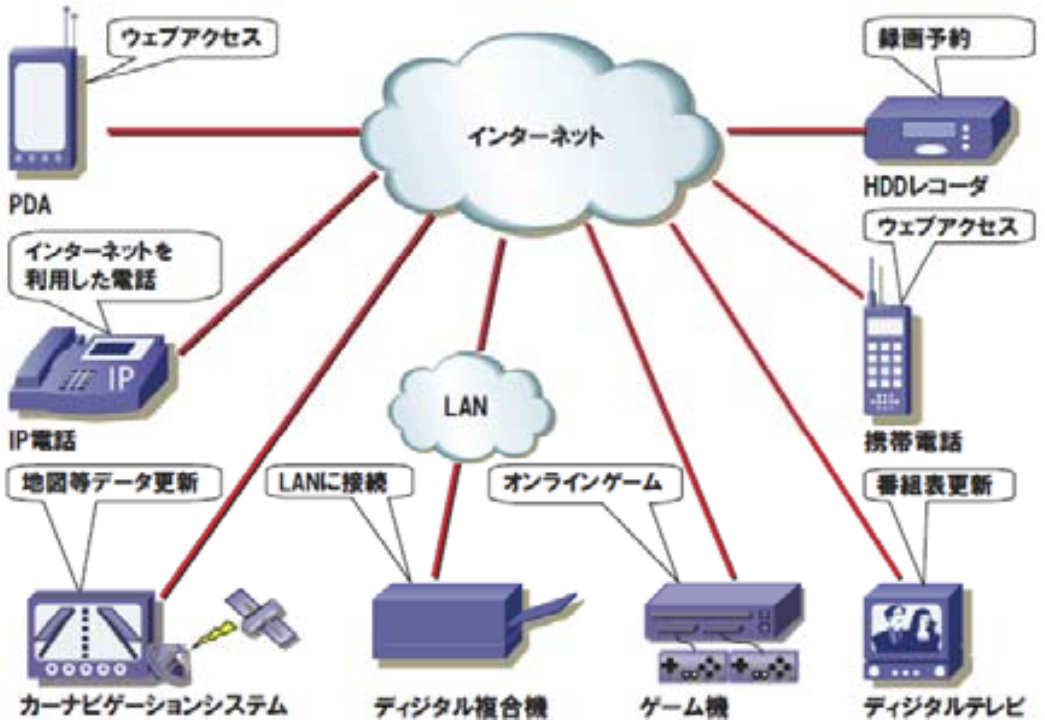
1．はじめに

1-1　市場動向と今後の懸念

□ あらゆる機器がネットワークへ繋がる時代
□ インターネットに接続するデジタルテレビの商品化が進む
□ 2011. 7の地上波デジタル放送への完全移行
□ IPv4のアドレス枯渇で、IPv6への移行加速

■ ネット接続製品での事故、事件事例
- 家庭用ルータがﾎﾞｯﾄｳｲﾙｽに感染
- DVDﾚｺｰﾀﾞの踏み台にされる脆弱性
- 組込み機器の管理用ｳｪﾌﾞに脆弱性

■ ネット、メディア利用が本格化した場合に想定されるセキュリティ問題をどうクリアしていくか



1-2 情報家電の課題

家電とPCの距離をいかに埋めていけるか、が大きな課題

利用者の特性		家電	＋ 情報家電	PC
ユーザ層		広く一般		広くなっているが、一般ではない
安全性への認識		安全		自己管理必要
（期待している）製品寿命		10～15年		5年程度
（外的）脅威の認識		なし（動かなければ故障）		あり（ウイルス、攻撃他）
セキュリティ対策	必要性の認識	なし		あり
	対策負担の理解	なし		あり
	対策のスキル	期待困難		あり（期待可能）

1-3 本報告書策定の経緯

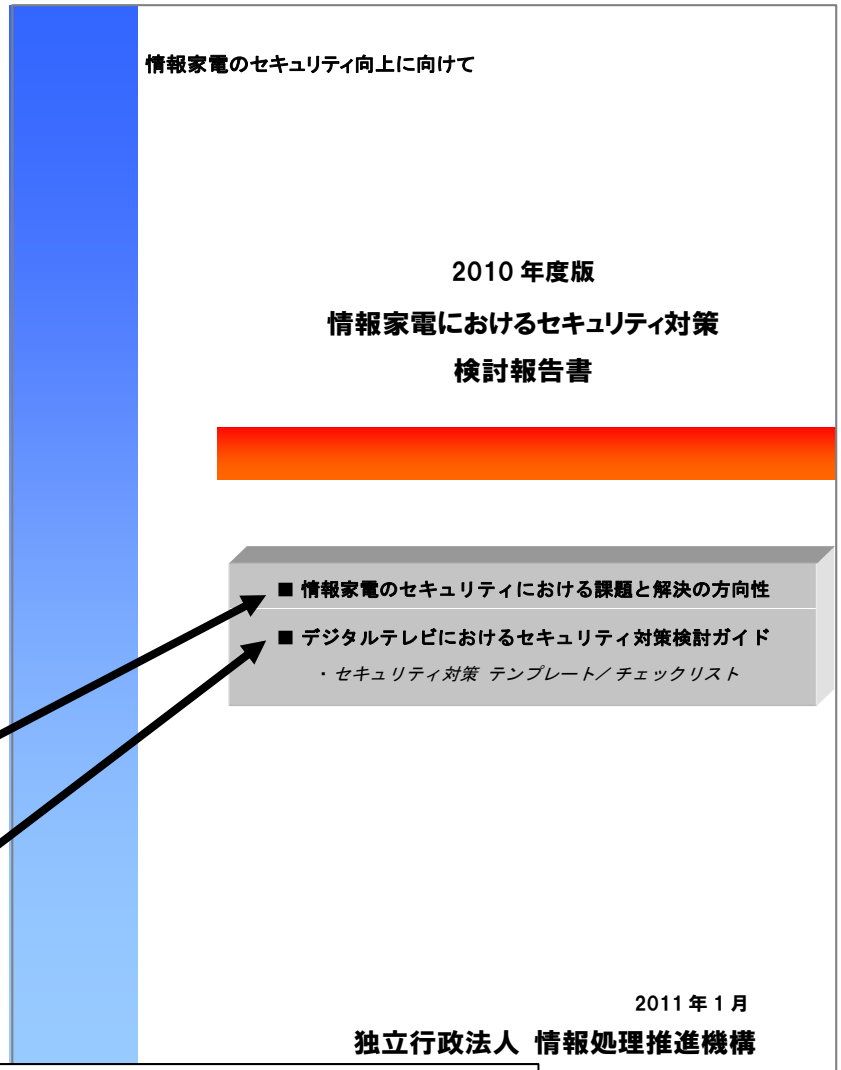
「情報家電セキュリティ勉強会」

1. 期間
2010年3月～12月； 7回の会議を実施

2. 出席
・家電各社： シャープ、ソニー、パナソニック、
日立ｺﾝｼｭｰﾏｴﾚｸﾄﾛﾆｸｽ、三菱電機 他
・オブザーバ： 経済産業省 情報セキュリティ政策室
・事務局： IPA セキュリティセンター

3. 経緯と成果
① 各社より、現状、課題を持ち寄って議論

② 市場が先行しているデジタルテレビを
対象に、脅威とセキュリティ対策を検討



http://www.ipa.go.jp/security/fy22/reports/electronic/index.html

2. 情報家電のセキュリティにおける課題と解決の方向性

2-1 情報家電のセキュリティにおける課題(1)

様々な意見・懸念 ⇒

課題	
	(1) 脅威の共通認識とセキュリティ対策の必要性
	(2) 情報家電市場形成の必要性
	(3) 業界としての連携、情報共有の必要性
	(4) 市場の牽引と発展

(1) 脅威の共通認識とセキュリティ対策の必要性

① 脅威の共通認識

- PCの環境に近付いており、PCで起っている脅威と同等の脅威の恐れ
- 汎用部品の利用により、 任意コードの実行といった深刻な脅威の高まり
- 製品の脆弱性対策を含めたアップデートには期間的な限界

② 業界の懸案、隘路

- 外部からくる脅威に対して、製品の安心、安全をどの程度、宣言できるのか
- 情報セキュリティに起因した事故時の責任範囲(分界点)のコンセンサス
- 設定ミスなどもセキュリティの脅威になる

③ 方向性: セキュリティ基準、ガイドライン、認証

- 業界で決めた基準的なものがあって初めて、ユーザも含めて不安が払拭される
- セキュリティ対策や脆弱性対応などの、合意されたガイドラインが必要である
- 基準もしくはガイドラインを満たしていることを、中立機関での認証が望ましい

2-2 情報家電のセキュリティにおける課題(2)

(2) 情報家電市場形成の必要性

① ユーザの状況

・安全との認識の家電において、セキュリティの脅威が一般消費者に理解困難
・安全な筈の製品に何故セキュリティ対策でお金をかけるのか、の理解困難

② 機器の利用面の隘路

・機器を正しく設定してもらえるか、取扱い説明書の記載で充分か
・情報家電で何か起った時、どうすれば良いのか、リテラシーの向上をどう図るか

③ 事故・故障対応

・事故や故障の原因として、設定不良、汚染や攻撃、改造や機能追加など、
その切り分けが困難であり、ユーザとの責任分界点の明確化も必要
・攻撃にあっていることや、自身が(踏み台等で)加害者になっていることに
気付かないケースへの対応も必要

④方向性: 市場形成

・各社で個別の説明をするのは難しく、業界で纏まったものが必要
・製品品質と脆弱性は本質的に異なっており、脆弱性を狙った攻撃で起きた
事故をどう捉えるか、市場としての共通認識が必要

2-3 情報家電のセキュリティにおける課題(3)(4)

(3) 業界としての連携、情報共有の必要性

① 業界としての連携

・ネット接続に伴って起りうる危険性を、業界で纏められることが望ましい
・脆弱性のレベルが軽微か、重大かの共通の尺度が必要

② 情報共有の必要性

・攻撃事例の共有、継続的に議論できる場や体制が必要
・脅威情報、脆弱性情報など、業界で共有できるニュートラルなDBが必要

(4) 市場の牽引と発展

① 市場の牽引

・コスト優先でセキュリティ対策レベルが低い情報家電が市場に出回るのは、消費者にとっても、市場形成からも好ましくない
・海外OEM生産品の受入れ検査基準も必要

② 国際標準、認証

・セキュリティ基準(ISO等)が必要。
・基準をクリアした製品が消費者に選択される市場の流れが必要

2-4 情報家電の課題と解決の方向性一覧

	課題
1	脅威の共通認識とセキュリティ対策の必要性
2	情報家電市場形成の必要性
3	業界としての連携、情報共有の必要性
4	市場の牽引と発展

解決の方向性
情報家電セキュリティ基準の確立
マーケットの育成（ベンダー）・リテラシーの向上（ユーザ）
情報DBの整備
グローバルデファクト・国際標準化への展開

表１．情報家電の課題と解決の方向性

#	課題 分類	課題 小項目	解決の方向性 対応項目	解決の方向性 目標
1	脅威の共通認識とセキュリティ対策の必要性	<脅威> ・プラットフォームに汎用部品が使われてきており、任意コードの実行といった深刻な脅威も高まっている。 ・情報家電がネットワークアクセスを含め、PCの環境に近付いており、PCで起っている脅威と同等の脅威に晒される恐れがある。 ・製品の脆弱性対策を含めたアップデートには期間的な限界（プラットフォームのサポート期限等）があるが、家電の10～15年におよぶ長期間利用にどう対応していくか。	情報家電セキュリティ基準	情報家電セキュリティ基準の確立
		<業界の脳路・懸案> ・企業として、外部からくる脅威に対してまで、製品の安心、安全をどの程度、宣言できるのか。 ・情報セキュリティに起因した事故時、メーカーの責任範囲のコンセンサスが必要となる。 ・設定ミスなどもセキュリティの脅威になるため、マニュアル、取扱説明書の記載レベルの基準が必要である。		
		<方向性： セキュリティ基準、ガイドライン、認証> ・業界で決めたセキュリティ対策上の基準的なものがあって初めて、ユーザも含めて不安が払拭される。 ・セキュリティ対策や脆弱性対応や暗号アルゴリズム選定のチェックリストや合意されたガイドラインが必要である。 ・中立機関による認証という仕掛けがあると望ましいが、極力コスト（認定期間含む）がかからない考慮が必要である。	認証・認定制度	
2	情報家電市場形成の必要性	<ユーザ状況> ・安全との認識の強い家電において、起りうるセキュリティの脅威が一般消費者に理解して頂くのが困難である。 ・PCはセキュリティ対策が必須という市場形成がなされてきているが、情報家電のユーザー層はそれより広範となる。 ・情報家電に対するセキュリティ意識は行き渡っておらず、どう説明、理解してもらい、リテラシーの向上を図るかが課題である。 ・安全な筈の製品に何故セキュリティ対策でお金をかけるのか、なかなか理解が得られない。	ネット接続機能利用で想定される脅威の理解	マーケットの育成（ベンダー） リテラシーの向上（ユーザ） 製品ライフサイクルへの対応
		<機器の利用面の脳路> ・取扱説明書には沢山書いてきているが、機器を正しく設定してもらえるかが課題である。 ・情報家電で何か起った時、どうすれば良いのか、機能利用だけでなくユーザのリテラシーの向上が重要である。	ユーザ意思による機能選定の認識	
		<事故・故障対応> ・事故や故障の原因として、設定不良、ネット接続利用、改造や機能追加など様々考えられ、その切り分けが困難であり、またユーザとの責任分界点の明確化が必要である。 ・ユーザーは攻撃にあっていることや、自身が（踏み台等で）加害者になっていることに気付かないケースもある。	利用時（廃棄フェーズも含む）の留意事項の徹底	
		<方向性： 市場形成> ・各社で個別にネット接続の注意事項、危険性をユーザに説明するのは難しく、業界で纏まったものが必要である。 ・製品品質と脆弱性は本質的に異なっており、脆弱性が原因でおきた事故をどう捉えるか、共通認識が必要である。	事故発生時の対応フローの整備・周知	
3	業界としての連携、情報共有の必要性	<業界としての連携> ・ネット接続に伴う危険性を各社が個別で出すのは難しく、業界で纏められることが望ましい。 ・脆弱性のレベルが軽微か、重大かの判断を各社がするのは難しく、共通の尺度が必要である	開発者向け情報DB	情報DBの整備
		<情報共有の必要性> ・攻撃事例の共有、継続的に議論できる場や体制が必要である。 ・脅威情報、脆弱性情報など、業界で共有できるニュートラルなDBが必要である。 DBは、開発者向けと、ユーザー向けのそれぞれのものが必要である。	ユーザ向け情報DB	
4	市場の牽引と発展	<市場の牽引> ・世界市場でコスト、機能における競争の中で、コスト優先でセキュリティ対策レベルが低い情報家電が市場に出回るのは、ユーザにとっても、市場形成からも好ましくない。 ・海外OEM生産品の使用が増える方向であるので、それらにどのような受入れ検査をすればよいかも課題となる。	セキュリティ基準の国際標準化	グローバルデファクト・国際標準化への展開
		<国際標準、認証> ・セキュリティ基準をISO等に提案して、それをクリアした、あるいは認証を受けた製品が消費者に選択される市場の流れを作るのが望ましい。	認証、認定制度の市場デファクト化	

2-5 情報家電の解決の方向性(1)

(1) 情報家電セキュリティ基準の確立

① 情報家電セキュリティ基準: 以下を規定する
- 保護すべき資産 、機能と、脅威の明確化
- 製品へのセキュリティ対策実装項目(利用機能によるレベル、段階が必要)
- 製造現場におけるセキュリティ管理体制
- 製品取扱い説明書への記載事項、記載レベルの明確化
- 発売後の運用スキーム(脆弱性対策など)
- 新しい技術(IPv6等)への対応

② 認証・認定制度: 以下の要件を満たす
- 家電業界の事業環境(世界競合、製品長寿命、新製品短期開発サイクル等)に適合
- コスト負担や審査プロセスが過負荷にならない形態
- それぞれの規模の事業者の事業展開に負担が大き過ぎない形態
- 製品の実情に基づいた自己宣言から、認証、認定シール貼付などのレベル
- 中立の第三者機関による認証・認定制度
- 製品の価値(信頼性、安全性等)として、認定取得が消費者に分かりやすい

2-6 情報家電の解決の方向性(2)

(2) マーケットの育成、情報家電リテラシーの向上

① ネット接続機能利用で想定される脅威の理解： 以下のアプローチ ・取扱説明書での記載内容(機能の利用と想定脅威の明記) ・パンフレット(広く周知させるための素材)　・公開Webサイト、教育素材
② ユーザ意思による機能選定の認識 ・取扱説明書の記載内容の規約(危険性、遵守事項、利用時対策などの記載) ・搭載機能の活性化の意思表示手段のルール化
③ 利用時(廃棄フェーズ含む)の留意事項の徹底 ・セキュリティアップデートの必要性の理解(上記②の取扱説明書での記載)と運用 ・ネット利用時に、アップデートへの誘導が図られるシステム仕様 ・廃棄時、機器上に残る情報消去手段の提示
④ 事故発生時の対応フローの整備 ・取扱説明書での記載内容の規約　・問合せ窓口　・対応するWebサイトの設置

2-7 情報家電の解決の方向性(3)(4)

(3)情報DBの整備

① 開発者向け情報DB
- 国内の脆弱性対策情報データベースであるJVN iPedia の活用
- 情報収集対象の拡大や使い勝手(I/F)の向上

② ユーザ向け情報DB
- 情報家電全般もしくは製品分野共通の脆弱性や脅威
- 注意喚起すべき事件・事故事例
- インシデント対応ノウハウ

(4)グローバルデファクト・国際標準への展開

① セキュリティ基準の国際標準化
- 業界がセキュリティ基準を策定、それに準拠することにより、デファクトの確立
- 国際標準にもっていく可能性を探る

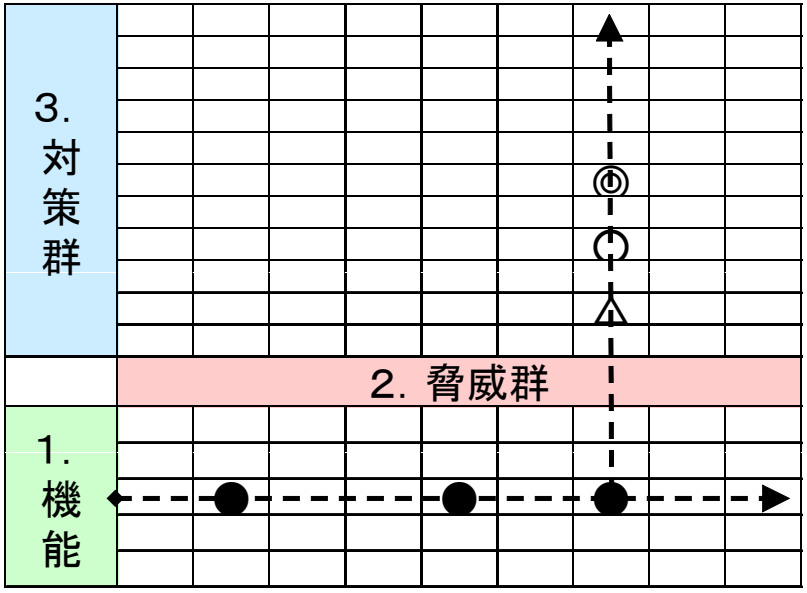
② 認証、認定制度の市場デファクト化
- 認証を受けた製品が、消費者に選ばれると流れを作る

3. デジタルテレビにおける
セキュリティ対策検討ガイド

3-1 アプローチ

① 情報家電セキュリティ基準： 以下を規定する
- 保護すべき機能、資産 と脅威の明確化
- 製品へのセキュリティ対策実装項目（利用機能によるレベル、段階が必要）

1. 搭載する情報利用機能の明確化
2. 機能と想定脅威の対応の明確化
3. 脅威と対策候補の対応の明確化



どの情報利用機能に
対して
どの対策を検討すべきか

3-2 デジタルテレビにおける情報利用機能

(1) 外部メディア利用機能

① 内蔵ドライブ　<→ A1>

DVD等を読み込むオプティカルドライブ

② 汎用インタフェース　<→ A2>

USBやEthernetなど、汎用外部接続インタフェース経由の接続

(2) 蓄積メディア内蔵　<→ B>

内蔵されているHDD（Hard Disk Drive）

(3) LAN接続

① 有線LAN　<→ C1>

Ethernet、PLCなどを介した家庭内の有線LAN

② 無線LAN　<→ C2>

IEEE802.11X、Bluetooth、ZigBeeなどを介した家庭内の無線LAN

(4) インターネット接続

① 特定サイト接続　<→ D1>

特定サイトか、特定サイトを介したサイトにのみインターネット接続

② 任意サイト接続　<→ D2>

通常のPCと同じ任意のサイトに接続が可能なインターネット接続

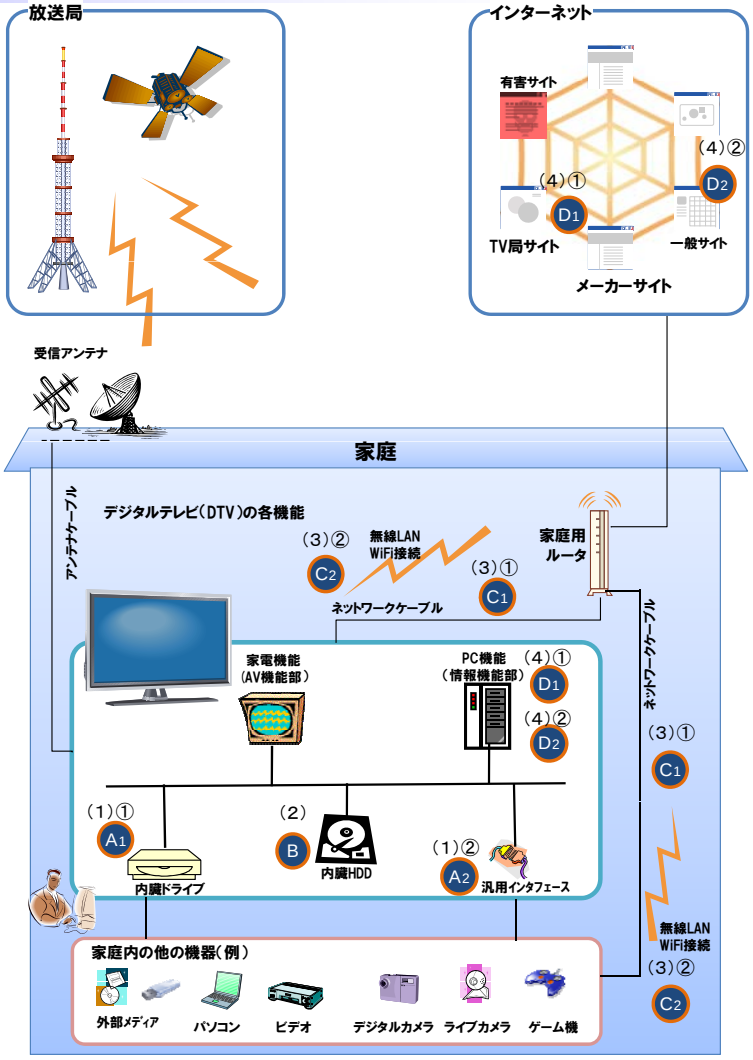


図1 デジタルテレビの構成概念図

（注）（n）○ は、3．1節の項番を、A1 ～ D2 は、3．1節表2左下の機能レベルの項番に対応

3-3　デジタルテレビにおける脅威 <1/2>

（1）媒体利用における脅威
　① ウイルス感染

（2）ユーザ操作上における脅威
　① 設定不良
　② 操作ミス
　③ 蓄積情報の漏えい（コンテンツ）
　④ 蓄積情報の漏えい（ユーザ情報）

（3）宅内における脅威
　① 不正利用（なりすまし）
　② 不正設定

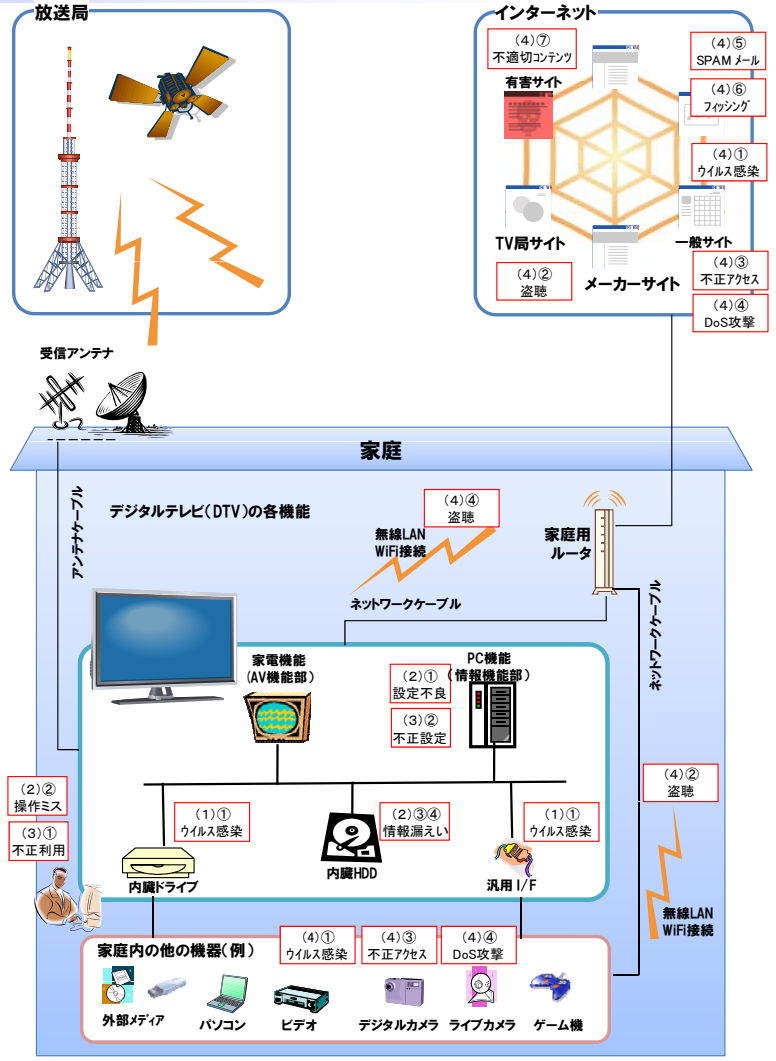


図2 デジタルテレビにおける脅威の全体像

（注1）（n）○ は、3．2節の項番を指している。
（注2）スペースが限られており、該当箇所に全ての脅威を記載していないので、詳細は表2を参照の事。

3-4　デジタルテレビにおける脅威 <2/2>

（4）ネット経由・ネット利用時
- ① ウイルス感染
- ② 盗聴
- ③ 不正アクセス
- ④ DoS (Denial of Service) 攻撃
- ⑤ スパム（SPAM）メール
- ⑥ フィッシング
- ⑦ 不適切コンテンツのアクセス

（5）　ポータルサイト側
- ① 端末／ユーザの成りすまし
- ② 一般Webと同等脅威
  - ・DoS攻撃、・不正アクセス、・ウイルス感染、
  - ・盗聴、・SPAMメール、・フィッシング、
  - ・Webアプリケーションの脆弱性への攻撃

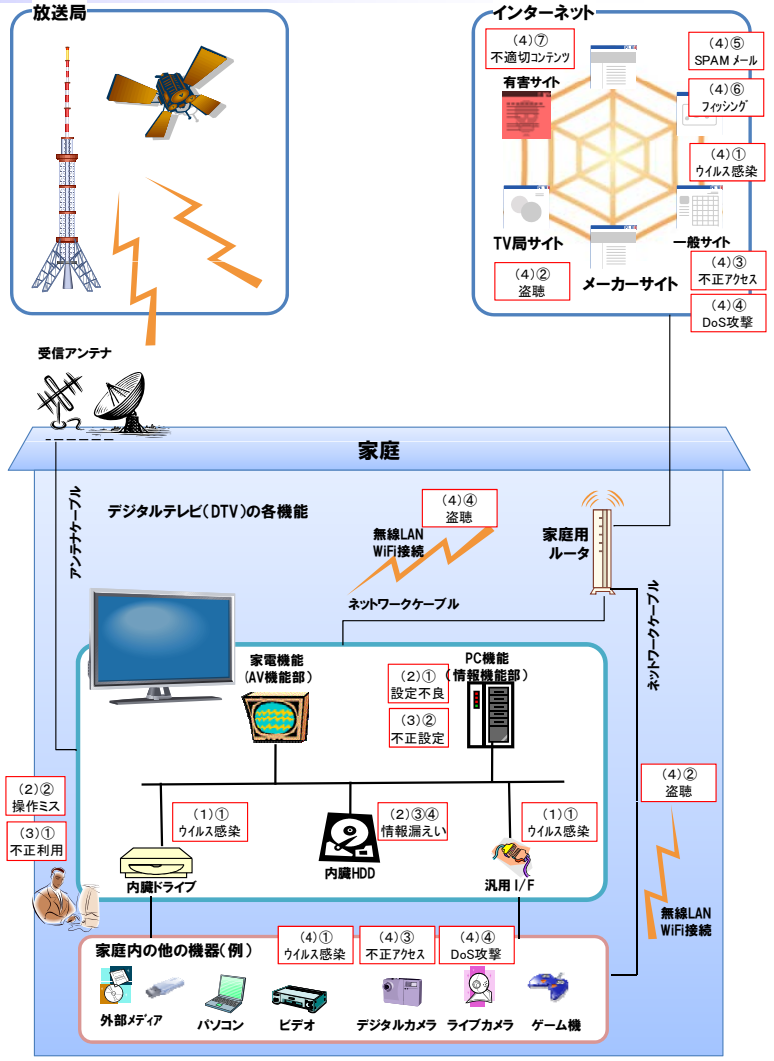


図2 デジタルテレビにおける脅威の全体像

（注1）（n）○ は、3．2節の項番を指している。
（注2） スペースが限られており、該当箇所に全ての脅威を記載していないので、詳細は表2を参照の事。

3-5　脅威に対する対策　＜1/2＞

(1) 脆弱性（セキュリティパッチ）対策　　＜→　1＞
　・インターネット接続サービス　　・放送波経由

(2) ファイアウォール（FW）　　＜→　2＞
　① 接続先特定（ルート制御）
　② 不正アクセス防御

(3) アンチウイルス　　＜→　3＞

(4) IDS／IPS (Intrusion Detection System／Intrusion Protection System)　＜→　4＞

(5) 通信路暗号化（VPN(Virtual Private Network))含む）　＜→　5＞
　① DTV機器と宅内機器の有線／無線でのネット経由
　② DTV機器と、インターネット経由外部Webサービス間
　③ DTV機器を使った外部ユーザ間

3-6 脅威に対する対策 ＜2/2＞

(6) 認証
- ① 機器認証 ＜→ 6＞
- ② ソフトウェア認証 ＜→ 7＞
- ③ ユーザ認証(対機器) ＜→ 8＞
- ④ ユーザ認証(対サービス) ＜→ 9＞
- ⑤ サーバ認証(対接続サーバ) ＜→ 10＞

(7) コンテンツ暗号化 ＜→ 11＞

(8) データ消去ツール ＜→ 12＞

(9) フィルタリングツール
- ① Webフィルタリング ＜→ 13＞
- ② メールフィルタリング ＜→ 14＞

(10) 取扱い説明書明記 ＜→ 15＞

・機能の選択 ・セキュリティパラメータの設定 ・セキュリティ運用(脆弱性対策など)
・機器異常時、故障／事故時の対応 ・廃棄時の対応

3-7 機能 → 脅威 → 対策一覧

15	取扱い説明書明記			○	○	○	○				○ 無線LAN向け							
14	フィルタリングツール	メール向け												○	○ メール			○	プロバイダサービスとして提供
13		URL 向け								○					○ サイトアクセス	○		○	プロバイダサービスとして提供
12	データ消去ツール					○ disk	○ flush												flushメモリ / Disk それぞれ
11	コンテンツ暗号化					△	△					△						○	
10	認証	サーバ(接続先)								△					○	△		○	
9		ユーザ(対サービス)				△ ネット経由	△	○	○							△	○	○	サービス側におけるユーザ認証
8		ユーザ(対機器)				○	○	○	○							△			機器の利用(ログイン)におけるユーザ認証
7		ソフトウェア	○							○									機器にインストールされるソフト(ドライバ含む)の認証
6		機器										△					○		サービス側の接続要求機器認証。機器ID, TPMなど
5	通信路暗号化(VPN含む)										○							○	Webサイト、プロバイダサービスとして提供
4	IDS/IPS									△		○	○					○	仮想パッチでウイルスにも対応
3	アンチウイルス		○							○								○	
2	ファイアウォール											○	○					○	ポート制御、接続先特定など
1	脆弱性(セキュリティパッチ)対策		○							○		○						○	衛星配信、もしくは、端末操作

対策 / 脅威(一次的) / 機能			媒体	ユーザ操作				宅内		ネット経由							ポータルサイト側		備考
			ウイルス感染	設定不良	操作ミス	蓄積情報漏えい		不正利用(なりすまし)	不正設定(侵入、保守時等)	ウイルス感染	盗聴(ネット利用時)	不正アクセス	DoS攻撃	メール(SPAM)	フィッシング	不適切コンテンツアクセス	端末 / ユーザ成りすまし	一般Webと同等脅威	
						コンテンツ	ユーザ情報												
	基本機能(デジタルTV機能)			○	○		○		○										
A1	外部メディア利用	内蔵ドライブ	△			○													DVD等のオプティカルドライブ
A2		汎用インタフェース経由	△			○				△		△	△						USB, Ethernet(IP)など
B	蓄積メディア内蔵					○	○												内蔵ハードディスク
C1	LAN	有線								△	△	△	△						機器間のケーブル接続
C2		無線		○						△	○	△	△						家庭内Hubルータ間
D1	インターネット接続	特定サイト		○	△	△ ネット経由	△ ネット経由	△	△	△	○	△	△	△	△	△	○	○	特定サイト側で対策してリスク低減
D2		任意サイト		○	△	○ ネット経由	○ ネット経由	○	△	○	○	○	○	○	○	○	—	—	

○:発生する可能性が高い、 △:発生する可能性がある、 (空欄):発生可能性はない　　:該当せず

3-8 本テンプレートの活用方法のご提案

テンプレート: 対象のデジタルテレビに搭載している情報機能に対して、横方向に想定される脅威を抽出し、その脅威に対して、縦方向に対応するセキュリティ策を抽出することが可能である。
その活用方法として、

(1) 商品の企画、設計時のセキュリティ対策のテンプレート
商品の企画、設計時において、どのようなセキュリティ対策機能を実装する必要があるかを検討するテンプレートとして用いる。

(2) 現製品のセキュリティ機能のチェックリスト
現製品に搭載している情報機能に該当する脅威と対策項目に対して、どのようなセキュリティ対策がなされているかを、○△のついた項ごとにチェックする。各項目に対して、該当製品に対応セキュリティ機能がある場合はその対策レベルを、あるいは、セキュリティ機能がない場合はその妥当性を検証する。

4. おわりに

4-1 情報家電プラットフォームに関わる脆弱性の届出の状況

■ 情報家電、組込み系のプラットフォームの脆弱性の届出が増えてきている

□ 情報家電、組込み系で使われるソフトもJVN iPediaの対象としていく
□ 必要に応じて、NVDからJVN iPediaへの吸収を推進する

AndroidのNVD, iPediaでの登録状況 ＜一部＞

分類	CVE	CPEベンダ	CPEプロダクト	iPedia登録
Androidモジュール（API、LIB、SDK含む）の脆弱性				
「Vulnerable software and versions※」にCPEの記載有				
	CVE-2009-0475	android	opencore	無
	CVE-2009-1754	android	android	無
	CVE-2009-2348	android	android	無
	CVE-2009-2656	android	android	無
	CVE-2009-2999	android	android	無
	CVE-2009-3698	android	android	無
	CVE-2009-0608	android	android sdk	無
	CVE-2008-0985	google	android sdk	無
	CVE-2008-0986	google	android sdk	無
	CVE-2009-0606	openhandsetalliance	android sdk	無
	CVE-2009-0607	openhandsetalliance	android sdk	無
「Vulnerable software and versions※」にCPEの記載無				
	CVE-2010-1807	apple	safari	有
	CVE-2009-1442	google	chrome	有
	CVE-2009-2692	linux	kernel	有

今月、JVN iPedia登録予定

4-2 情報家電プラットフォームに関わる脅威の届出の状況

■ 情報家電、組込み系のプラットフォームを標的にしたウイルスが増えてきている。
■ 今後、情報家電、携帯端末で、付加価値の高いサービスが増えるに伴って攻撃も増加が予想される

＜ベンダーおよびユーザ の両輪での対策、対応が重要である＞

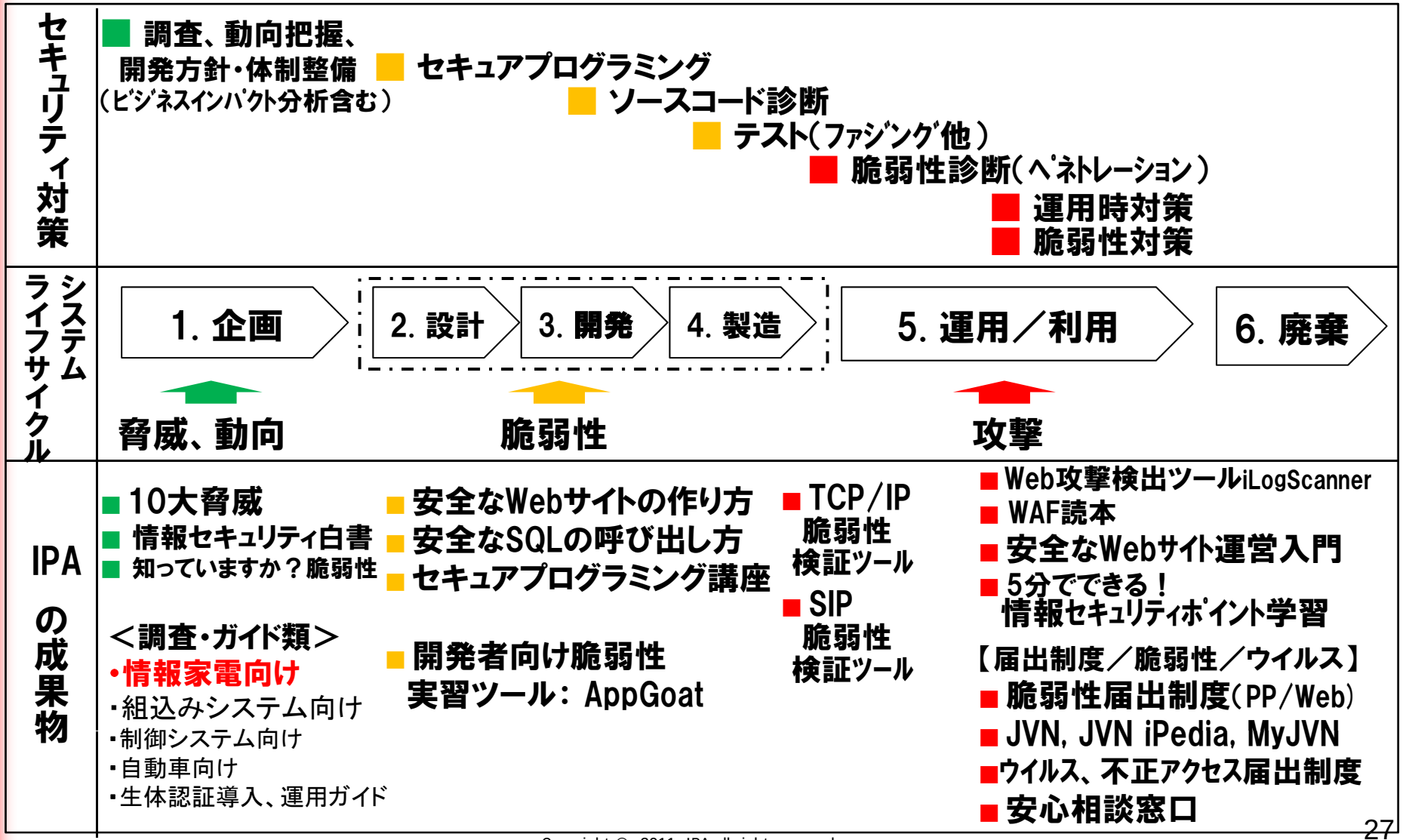
□ サービス内容、システム形態適合したセキュリティ対策の考慮
□ 適切なセキュリティ情報の提供、注意喚起によるユーザの対応

Android OSを標的としたウイルスに関する注意喚起　第11-04-206号掲載日：2011年1月21日
http://www.ipa.go.jp/about/press/20110121_2.html

	発生時期	種類	特徴
1	2010年8月頃	トロイの木馬	有用なアプリに見せかけ、ひそかにSMS（ショートメッセージサービス）を悪用するトロイの木馬型ウイルスがAndroid Market※外で流通しました。
2	2010年8月頃	スパイウェア	ゲームアプリに見せかけ、端末に搭載されたGPSによる位置情報を第三者へ定期的に送信するスパイウェア型ウイルスがAndroid Marketで公開されていました。
3	2010年末～現在	ボット	正規のアプリにボット型ウイルスが抱き合わされた不正なアプリが、第三者の（Android Market外の）アプリ配布サイトで公開されています。

※ Android Market：Google社が運営している、Android用のアプリを配信、販売するサービス

4-3　脆弱性のない安全なシステム開発、環境に向けたIPAの取組み



Copyright ©　2011, IPA all right reserved.

参考

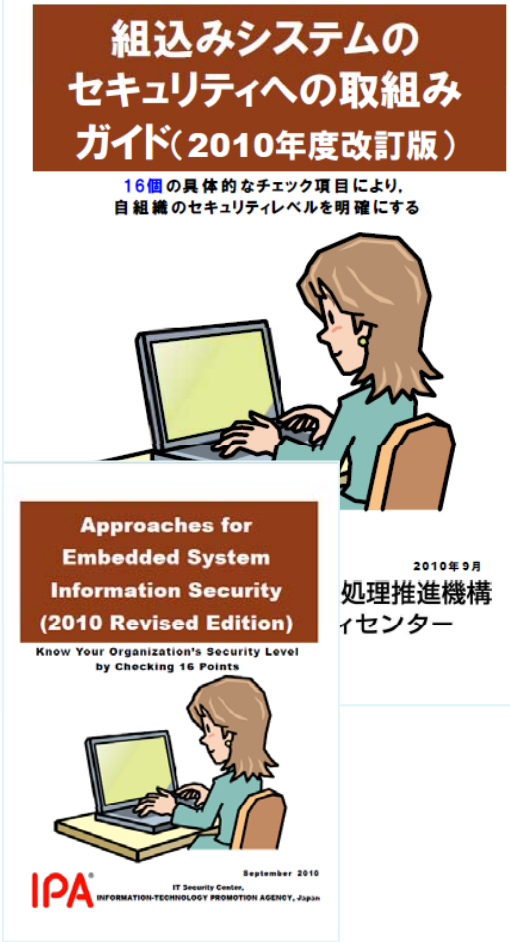
組込みシステムのセキュリティへの取組みガイド

http://www.ipa.go.jp/security/fy22/reports/emb_app2010/

16の具体的なチェック項目と4つのレベル

●「マネジメント」、「企画」、「開発」、「運用」、「廃棄」の**全てのフェーズを網羅**

●各フェーズからセキュリティのために重要な計**16項目**を選定し、項目ごとに**4つのレベル**を策定。



本書の活用法

- 自組織の把握
- 上位を目指す
- よりセキュアな製品

項目ごとのレベルが一覧できる付録チェック表
（「マネジメント」「企画」フェーズのみ抜粋）

ライフサイクル（マネジメントを含む）		「セキュリティへの取組み」のレベル			
段階(フェーズ)	セキュリティを考慮すべき項目	レベル1	レベル2	レベル3	レベル4
マネジメント	1-1. セキュリティルール (P.13)	・セキュリティルールの策定は行っていない	・セキュリティルールは開発者が自主的に策定している ・セキュリティルールは開発責任者や担当者主導で策定される	・組織としてセキュリティルールを策定し、規則集として明文化している	・組織としてセキュリティルールを策定し、規則集として明文化しており、担当者が規則を順守していることを確認するための手段も規定している
	1-2.セキュリティ教育 (P.15)	・セキュリティ教育は実施していない	・セキュリティに関する分科会（小集団活動）が自主的に活動している ・必要に応じて開発責任者や開発者主導で知識を習得したり、勉強会が行われたりする	・セキュリティ教育が業務に組み込まれている ・セキュリティに関する講習会や研修の受講が奨励される	・セキュリティ教育が業務に組み込まれている ・専門家による研修カリキュラムが義務付けられている
	1-3.セキュリティ情報の収集 (P.17)	・セキュリティ情報は特に収集していない	・開発責任者や開発者主導で必要に応じて情報収集を行っている	・組織として情報収集を行い、収集結果は開発者に伝達される仕組みを構築している	・脆弱性情報ハンドリングに積極的に関与し、脆弱性関連情報の活用に努めている
企画	2-1.予算 (P.18)	・セキュリティに係る予算は用意されていない	・プロジェクトリーダー（開発責任者）の要求があった場合に、予算確保が容認される ・開発責任者や開発者から要求があった場合に、検討される	・開発プロセスの一つとしてセキュリティ確保のために一定の基準で予算を割り振ることが前提として組まれている	・組織にセキュリティ部門等を設置するための予算を確保し、活動する
	2-2.開発プラットフォーム選定 (P.19)	・コスト優先、納期優先で選定され、セキュリティについてはほとんど考慮されない	・開発時に判明している脆弱性への対策は実施する ・出荷後は特に実施されない ・開発プラットフォームの選定を実施する担当者または部門がない ・その製品の開発責任者や開発者によって脆弱性対策の意識が異なり、組織として統一した取組みはなされない	・組込みソフトウェアパッケージを利用する場合、販売元からの脆弱性対策プログラム等のリリース情報を監視している ・出荷後の製品に対してもソフトウェアアップデート等によって対策を実施している ・同じ製品を扱う部門内では脆弱性対策への意識が高く、統一した取組みがなされている	・全社的に脆弱性対策を実施している ・出荷後の製品に対してもソフトウェアアップデート等によって対策を実施している ・販売元の脆弱性対策に関するサポート体制について事前に確認を行う ・デバイスや回路構成においてセキュリティを考慮した選定を行っている ・製品のセキュリティを高める目的で、独自のプラットフォームの開発や調達先への改善要求活動などを実施している

Copyright © 2011, IPA all right reserved.

参考

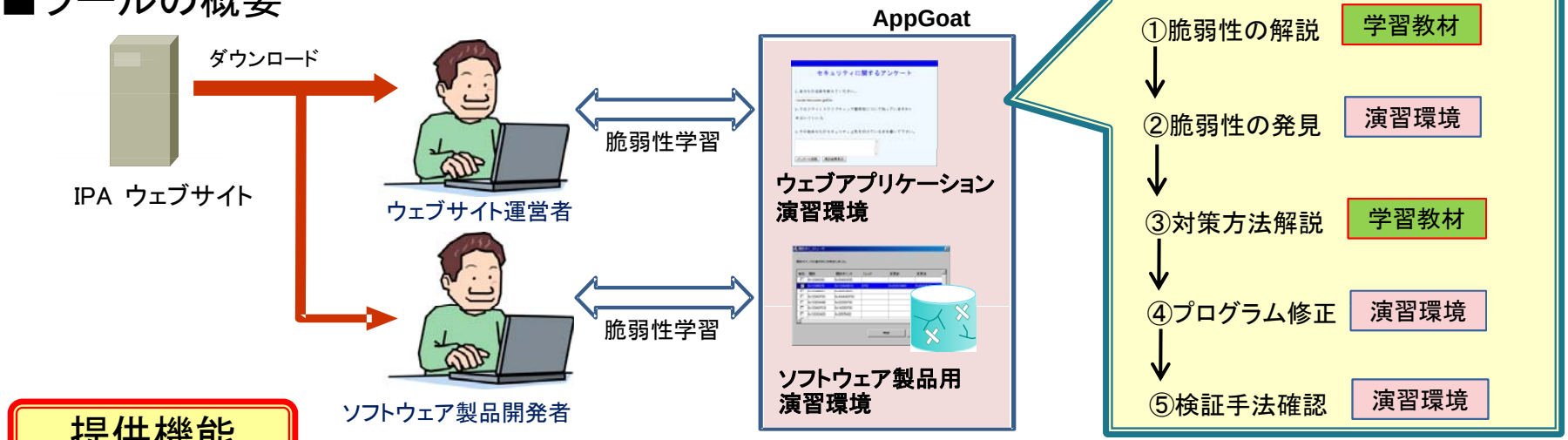
『脆弱性体験学習ツール AppGoat』

http://www.ipa.go.jp/security/vuln/appgoat/index.html

■概要

ウェブサイト運営者やソフトウェア製品の開発者が脆弱性対策の必要性及び対策手法等を演習環境で体験的かつ実践的に学ぶツール「脆弱性体験学習ツール」を2011年1月27日に公開しました。

■ツールの概要



提供機能

- **ウェブアプリケーション演習環境**
  - 演習用に準備された故意に脆弱性を持たせた擬似的なウェブサイト
- **ソフトウェア製品用 演習環境**
  - 演習用に準備された故意に脆弱性を持たせた、擬似的なサーバ及びデスクトップアプリケーション等の集合
- **学習教材**
  - 利用者の演習の補助や理解・知識を深めるための教材

Copyright © 2011, IPA all right reserved.

参考

『脆弱性体験学習ツール AppGoat』

http://www.ipa.go.jp/security/vuln/appgoat/index.html

■開発の背景

- 近年、ウェブサイトや国産のソフトウェア製品の脆弱性を突いた攻撃や被害が多数報告されている。しかし、既に公表されている脆弱性（既知の脆弱性）の対策が実装されていないケースや、脆弱性が「再発」するケースが少なくない。
- 脆弱性対策の習得には、学習者自らが演習しながら学ぶのが効果的であるが、国内では演習環境が整備されていないこともあり、脆弱性対策・検証技術を習得する場が少ない。
- 海外ではウェブアプリケーション環境に限り、演習形式で学習できるツールが整備・提供されているが、英語表示である為、学習のハードルが高くなってしまう。

セキュアな「設計」「実装」「検証手法」を一連の演習を通して学習できるツールの開発・提供

■期待する効果

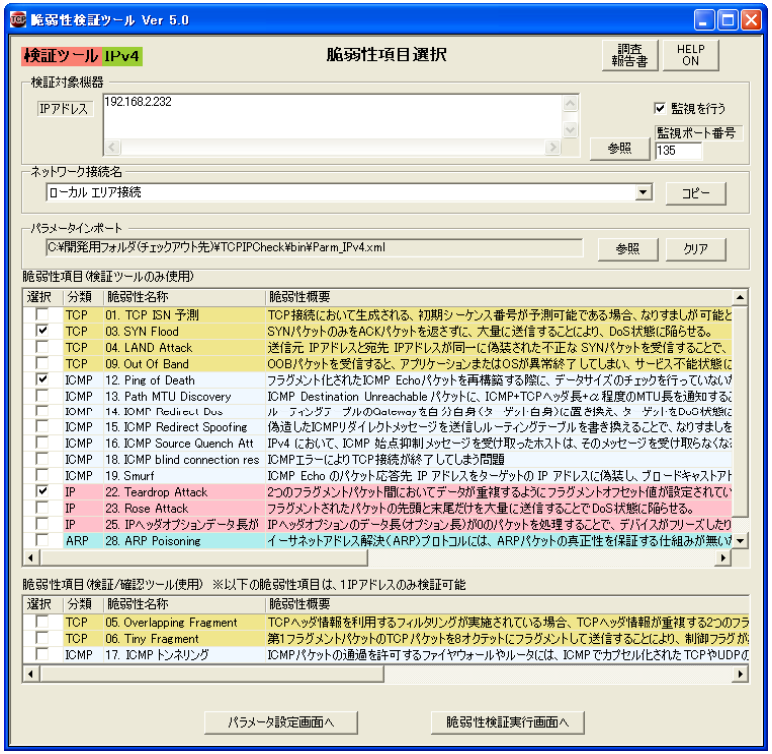
- **セキュア開発の促進**
  - ソフトウェア開発者が本ツールを通して「設計」「実装」「検証手法」を学習できることで、セキュア開発の促進を期待。
- **セキュリティ検査の周知・促進**
  - 本ツールで脆弱性検証手法を学習できることで、製品ベンダーが出荷前のセキュリティ検査の促進を期待。
- **ウェブサイト運営者への啓発**
  - セキュリティ意識の低いウェブサイト運営者が本ツールで学習することで、脆弱性により引き起こされる被害を実体験でき、対策促進を期待。

Copyright © 2011, IPA all right reserved.

参考

TCP/IPに係る既知の脆弱性検証ツール

http://www.ipa.go.jp/security/vuln/vuln_TCPIP_Check.html



TCP/IPに係る脆弱性を検証

- TCP/IPに係る既知の脆弱性に関する**調査報告書を公開**
- TCP/IP利用機器に対して自動的に検証を実行し、脆弱性の有無について簡易判定が可能
- 調査報告書に記載されている30項目のうち、**IPv4で19項目、IPv6環境で14項目の脆弱性をツールにて検証可能**
- 調査報告書を参照することにより、脆弱性の有無をより正確に判断可能

■ 利用申し込み方法

次のメールアドレスに、メールで申し込み

vuln-inq@ipa.go.jp

詳しくは、次のウェブサイトを確認してください

http://www.ipa.go.jp/security/vuln/vuln_TCPIP_Check.html

●貸出数

貸出開始からの累計で、約120件の貸出実績

IPA 人気ツール

Copyright © 2011, IPA all right reserved.

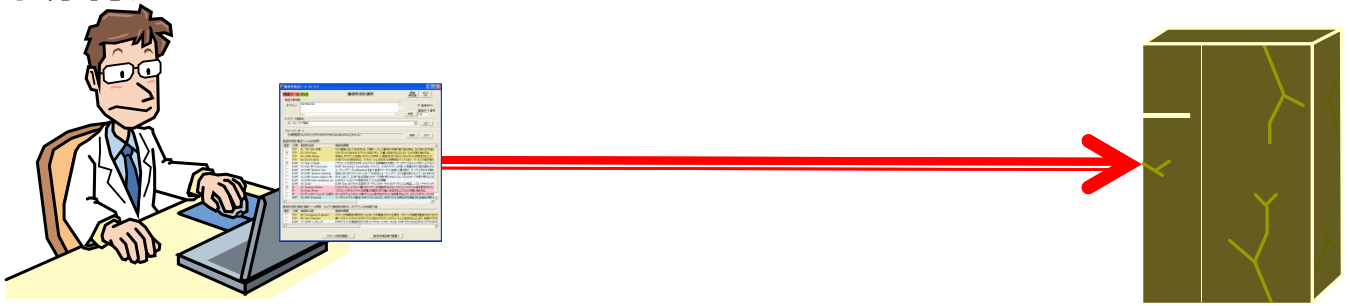
参考

TCP/IPに係る既知の脆弱性検証ツール

http://www.ipa.go.jp/security/vuln/vuln_TCPIP_Check.html

利用イメージ

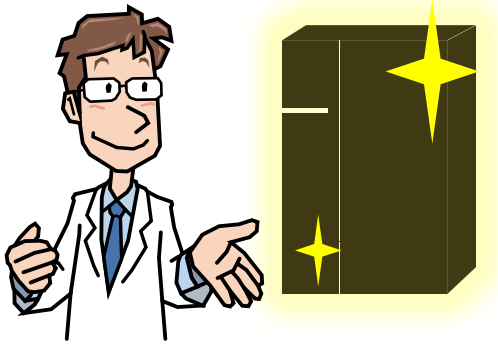
① 「TCP/IPに係る既知の脆弱性検証ツール 」を用いて、脆弱性の有無について簡易判定する



製品開発者　　TCP/IPスタックを実装した製品

② 「TCP/IP に係る既知の脆弱性に関する調査報告書」を確認することで、脆弱性の有無をより正確に判断する

③ 検出された脆弱性を修正する



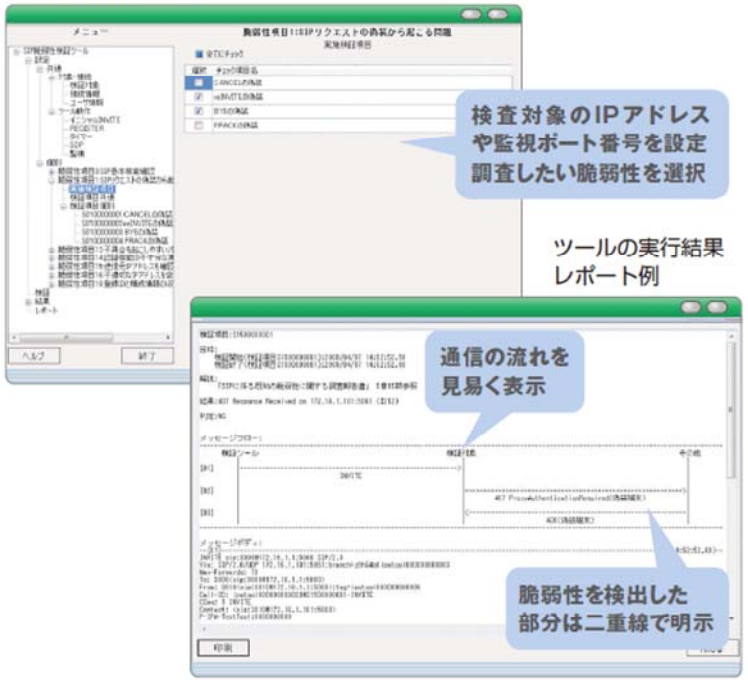
Copyright © 2011, IPA all right reserved.

参考

SIPに係る既知の脆弱性検証ツール

http://www.ipa.go.jp/security/vuln/vuln_SIP_Check.html

ツールの実行画面例



SIPに係る脆弱性を検査。

- SIPに係る既知の脆弱性に関する**調査報告書を公開**
- SIPを実装したソフトウェアに対して検証を実行し、脆弱性の有無について簡易判定が可能
- 調査報告書に記載されている22項目のうち、**11項目（265シナリオ）の脆弱性検査が可能**
- 調査報告書を参照することで、脆弱性の内容と対策方法

■ 利用申し込み方法

次のメールアドレスに、メールで申し込み

vuln-inq@ipa.go.jp

詳しくは、次のウェブサイトを確認してください

http://www.ipa.go.jp/security/vuln/vuln_SIP_Check.html

●貸出数

貸出開始からの累計で、約30件の貸出実績

専門家に好評なツール

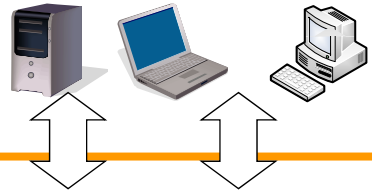
Copyright © 2011, IPA all right reserved.

参考

脆弱性対策情報ポータルサイト
（JVN、JVN iPedia、MyJVN）

1. 企画 | 2.設計 | 3.開発 | 4.製造 | 5.運用／利用 | 6.廃棄

- 国際性と地域性とを兼ね備えたデータベースと国際的な共通基準を用いた機械処理基盤の連携



MyJVN　CVE、CPE、CWE、CVSSなど共通基準を用いた情報共有フレームワークサービス（MyJVN API）の提供

JVN(JVN#12345678)
Vulnerability Handling Coordination Database

	日本語サイト http://jvn.jp/	英語サイト http://jvn.jp/en/
情報セキュリティ早期警戒パートナーシップ	情報セキュリティ早期警戒パートナーシップ案件（約466）	翻訳 → 情報セキュリティ早期警戒パートナーシップ案件（約400）
CERT/CC CPNI	CERT/CC、CPNI案件(約300)	蓄積 → JPCERT/CC

JVN iPedia(JVNDB-yyyy-0123456)
Vulnerability Archiving Database

	日本語サイト http://jvndb.jvn.jp/	英語サイト http://jvndb.jvn.jp/en/
JVN	JVN案件（995件）	蓄積 → JVN案件（481件）
日本国内製品開発者サイト	日本国内製品開発者案件（116件）	翻訳 → 日本国内製品開発者案件（116件）
NVD(英語)（約45,000）	NVD（8,516件）	（9,627件）（597件） IPA

2010年12月末の登録件数

Copyright © 2011, IPA all right reserved.

参考

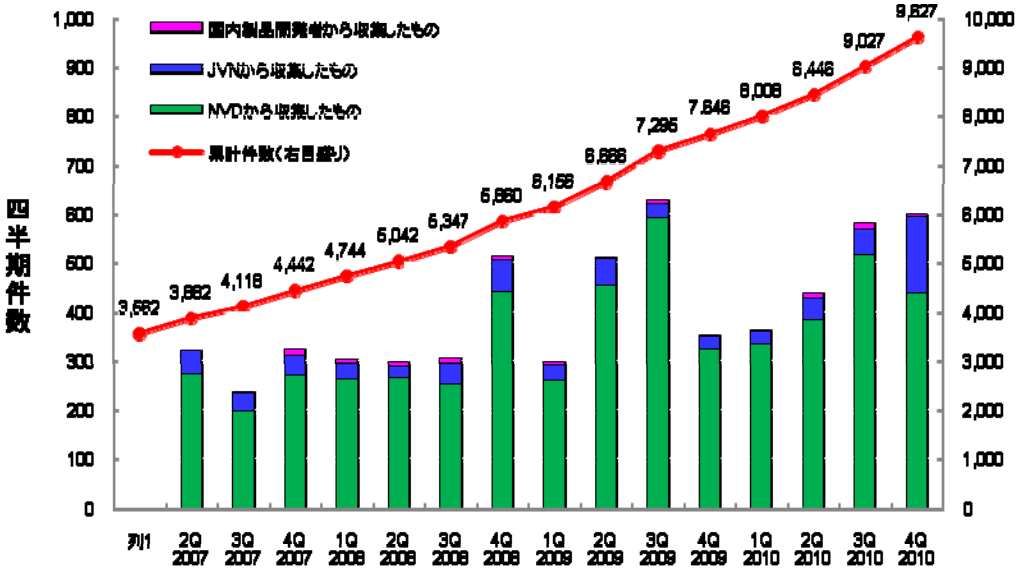
脆弱性低減における取組み

～脆弱性対策情報データベース（JVN iPedia）の運営～

1. 企画 | 2.設計 | 3.開発 | 4.製造 | 5.運用／利用 | 6.廃棄

- JVN iPediaとは？

  国内で利用されるソフトウェア等の製品(OS、アプリケーション、ライブラリ、組込み製品など)の脆弱性対策情報を中心に収集・蓄積する**脆弱性対策情報データベース**です。約9,600件の脆弱性情報蓄積しています。



JVN iPediaの登録件数の四半期別推移(2010/12末時点)

JVN iPedia登録件数(2010/12末時点)

	情報の収集元	2010 4Q	累計
日本語版	国内製品開発者	6件	116件
	JVN	156件	995件
	NVD	438件	8,516件
	計	600件	9,627件
英語版	国内製品開発者	6件	116件
	JVN	31件	481件
	Total	37件	597件

Copyright © 2011, IPA all right reserved.

IPAの提案する
デジタルテレビにおけるセキュリティ対策検討ガイド
の紹介

ご静聴、有難うございました。

独立行政法人　情報処理推進機構　セキュリティセンター
http://www.ipa.go.jp/security/index.html
http://www.ipa.go.jp/security/vuln/index.html